UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 8 Examination in Engineering: December 2025

Module Number: EC8204 **Module Name: Blockchain and Cyber Security (C-18)**

[Two Hours]

[Answer **all questions,** each question carries **10 marks]**

Q1 a) Bitcoin and Ethereum are two blockchain frameworks used in cryptocurrencies, with distinct design goals and mining mechanisms.

i) State THREE key differences between Bitcoin and Ethereum.

[1.5 marks]

ii) Define the following terms related to Bitcoin fundamentals:

- Hash Rate (q)
- Target (T)
- Common Prefix (k)

[1.5 marks]

iii) Explain why Bitcoin adjusts its mining difficulty every 2016 blocks. Write the target adjustment formula and explain each of its components.

[2.0 marks]

b) Blockchain technology manages and verifies data in a distributed network.

i) List THREE key properties that define blockchain technology.

[0.5 marks]

ii) Explain the following cryptographic components used in blockchain with examples:

- Hash functions - State two properties
- Digital signatures - State two purposes
- Public key cryptography - State one primary objective

[2.5 marks]

iii) A blockchain address is derived from a public key. Using Bitcoin as an example, illustrate how a blockchain address is calculated from a public key.

[0.5 marks]

iv) Consider a Merkle tree with 8 transaction hashes (T1 to T8) at the leaf level.

- Draw the structure of this Merkle tree showing all levels.
- Explain how a light client can verify that a specific transaction (e.g., T1) is included in a block without downloading all Transactions, by tracking through the path which includes T1 and considering sibling hashes of the same level.

- Calculate the minimum number of hashes required to perform this verification.

[1.5 marks]

Q2 a) Blockchain systems have been known to be vulnerable to attacks.

i) Define the THREE key security goals in blockchain systems.

[1.5 marks]

ii) Explain the double-spend attack in a blockchain system by addressing the following points:

- How the attack exploits network delay
- Why simple fixes (cancel both transactions, accept first received) fail
- Two effective mitigation strategies

[2.0 marks]

iii) A blockchain network consists of 100 nodes. Calculate the maximum number of adversarial nodes that can be tolerated under the following instances, and show your calculations:

- Bitcoin's security assumption
- Practical Byzantine Fault Tolerance (PBFT) consensus mechanism

Explain why PBFT requires a higher number of nodes for the same level of fault tolerance

[1.5 marks]

b) Blockchain systems make use of consensus approaches.

i) State the purpose of consensus mechanisms in blockchain and list TWO types of consensus approaches other than Proof of Work (PoW) or Practical Byzantine Fault Tolerance (PBFT).

[1.0 mark]

ii) Write the pseudocode for the PoW mining process. Your pseudocode should include:

Input parameters (s = previous block hash, x = Merkle root, T = target)

- The iterative hashing process
- The condition for a valid block
- Broadcasting the result

[2.0 marks]

iii) Explain the transition from Proof of Work to Proof of Stake (PoS) by addressing the following:

- The original PoW equation
- The final PoS equation after removing the nonce and Merkle root
- Two advantages of PoS over PoW
- One security challenge unique to PoS

[2.0 marks]

Q3 For each of the following statements, indicate whether it is ***True*** or ***False***. Provide a brief explanation of your answer in no more than 100 words. Your explanation should clearly justify your choice, highlighting the reasoning and/or any relevant concepts.

a) Domain Name System (DNS) zone transfers are considered a form of passive intelligence gathering method during penetration testing.

b) Shellcode written for a Linux 32-bit target to exploit a buffer overflow vulnerability will function correctly on a Linux 64-bit target.

c) The Same-Origin Policy prevents scripts on a malicious website from reading sensitive data from your banking website, even when both sites are open in different browser tabs.

d) Using a properly configured VPN eliminates the need for endpoint security solutions like antivirus software and firewalls.

e) Data privacy risks in AI systems are eliminated once the original training dataset is deleted after model training.

[5 x 2.0 marks]

Q4 a) Consider the network diagram shown in Figure Q4.a).

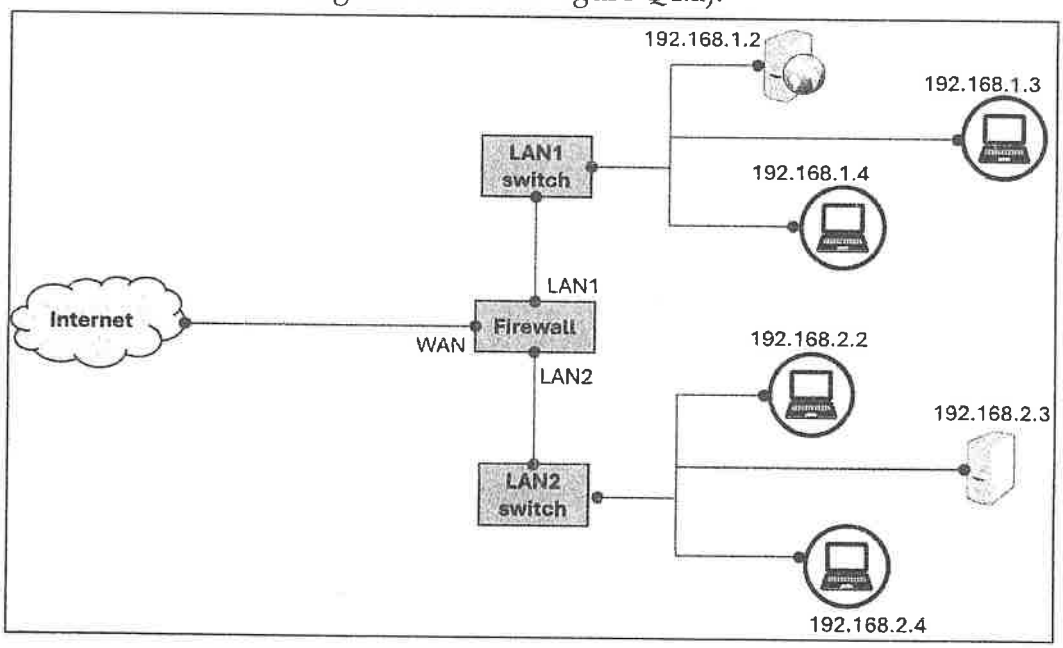

Figure Q4.a): Network diagram

WAN: 192.168.111.34
LAN1: 192.168.1.1
LAN2: 192.168.2.1

The security policy to be implemented at the firewall is as follows.

- The webserver (HTTP) 192.168.1.2 should be reachable by any internal or external host.

- The host 192.168.2.3 should be reachable over SSH (port 22) by LAN2 hosts only.
- Any internal host from LAN1 or LAN2 should be able to reach and communicate with external webservers (HTTP or HTTPS).
- All other traffic should be blocked.

Complete a stateful firewall using the table below, to implement the above security policy.
Note: You are required to draw the table in your answer script and fill it in.

Rule	Incoming interface	Source IP	Destination IP	Source port	Destination port	Protocol	State	Action

[4.0 marks]

b) i) What is port scanning, and what is its purpose in penetration testing?

[1.0 mark]

ii) Explain the differences between TCP SYN and TCP connect port scanning.

[2.0 marks]

c) i) What is a supply chain attack?

[1.0 mark]

ii) List TWO methods that can help minimize the risk of supply chain attacks.

[2.0 marks]